CLAIMS

1. A tamper-resistant security device having means for storing user credentials, including at least a security key, an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key, and means for external communication,

wherein said tamper-resistant security device further comprises:

- an application adapted for cooperating with said AKA module; and
- means for interfacing said AKA module and said cooperating application.

2. The tamper-resistant security device according to claim 1, wherein said cooperating application includes at least one of a security enhancing application and a privacy enhancing application.

3. The tamper-resistant security device according to claim 1, wherein said cooperating application is configured for performing enhanced security processing of at least one parameter associated with said AKA process.

4. The tamper-resistant security device according to claim 3, wherein said enhanced security processing includes at least one of:

- pre-processing of at least one AKA input parameter; and
- post-processing of at least one AKA output parameter.

5. The tamper-resistant security device according to claim 3, wherein said enhanced security processing includes encapsulation of said at least one AKA parameter.

6. The tamper-resistant security device according to claim 3, wherein said cooperating application is configured for receiving at least one AKA parameter from

said AKA process to generate a further AKA parameter that has higher security than said received AKA parameter.

7. The tamper-resistant security device according to claim 3, wherein said enhanced security processing includes evaluation of a predetermined number of consecutive AKA input parameters for verifying that said AKA input parameters can be used securely.

8. The tamper-resistant security device according to claim 7, wherein said enhanced security processing includes comparison of a predetermined number of consecutive AKA input parameters for verifying that all of said AKA input parameters are unique.

9. The tamper-resistant security device according to claim 8, wherein said enhanced security processing further includes combination of a predetermined number of consecutive AKA output parameters generated in response to a number of corresponding unique AKA input parameters.

10. The tamper-resistant security device according to claim 1, further comprising means for performing security policy processing based on information representative of security conditions in relation to said tamper-resistant security device.

11. The tamper-resistant security device according to claim 10, wherein the security conditions reflect at least one of the environment in which said security device is operated and the network interface over which a request for AKA processing originates.

12. The tamper-resistant security device according to claim 10, wherein said security policy processing includes at least one of a security policy decision process and a security policy enforcement process.

13. The tamper-resistant security device according to claim 10, wherein said means for performing security policy processing comprises means for selectively disabling direct access to said AKA module.

14. The tamper-resistant security device according to claim 10, wherein said tamper-resistant security device comprises means for detecting security conditions in relation to said tamper-resistant security device.

15. The tamper-resistant security device according to claim 14, wherein said means for detecting security conditions comprises means for detecting whether said tamper-resistant security device is operated in its normal environment or in an environment considered insecure, and said means for performing security policy processing comprises means for disabling direct access to said AKA module when operated in said insecure environment.

16. The tamper-resistant security device according to claim 1, wherein said cooperating application includes a security enhancing application, and said security device further comprises means for transferring a request for AKA processing directly to said AKA module if said security device is operated in an environment considered secure, and means for transferring said request to said security enhancing application if said security device is operated in an environment considered insecure.

17. The tamper-resistant security device according to claim 1, wherein said cooperating application is configured for performing at least part of the computations in connection with end-to-end key agreement between users.

18. The tamper-resistant security device according to claim 1, wherein said cooperating application is configured for masking key information generated by said AKA module.

19. The tamper-resistant security device according to claim 1, wherein said cooperating application is a software application installed in an application environment of said tamper-resistant security device.

20. The tamper-resistant security device according to claim 19, wherein input data is transferred to said cooperating software application by means of an existing command for accessing the application environment.

21. The tamper-resistant security device according to claim 19, wherein said application is securely downloaded into said tamper-resistant security device from a trusted party.

22. The tamper-resistant security device according to claim 1, wherein said cooperating application is a privacy enhancing application which participates in managing a user pseudonym.

23. The tamper-resistant security device according to claim 22, wherein said privacy enhancing application is configured for requesting an AKA response from said AKA module based on an old user pseudonym and for generating a new user pseudonym based on the received AKA response.

24. A tamper-resistant security device having means for storing user credentials, including at least a security key, an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key, and means for external communication,

wherein said tamper-resistant security device further comprises a software application implemented in an application environment of said tamper-resistant security device and adapted for cooperating with said AKA module, and said AKA module is also implemented, at least partly, as a software application in said application environment.

25. The tamper-resistant device according to claim 24, wherein said AKA software application and said AKA cooperating software application are at least partly integrated.

26. A user terminal provided with a tamper-resistant security device, said tamper-resistant security device having means for storing user credentials, including at least a security key, an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key, and means for communication with said user terminal,

wherein said tamper-resistant security device further comprises:

- an application adapted for cooperating with said AKA module; and
- means for interfacing said AKA module and said cooperating application.

27. The user terminal according to claim 26, wherein said cooperating application is at least one of a security enhancing application and a privacy enhancing application.

28. The user terminal according to claim 26, wherein said cooperating application is configured for performing enhanced security processing of at least one parameter associated with said AKA process.

29. The user terminal according to claim 28, wherein said enhanced security processing includes encapsulation of said at least one AKA parameter for producing an output parameter of higher security than said at least one AKA parameter.

30. The user terminal according to claim 26, further comprising means for performing security policy processing based on information representative of security conditions in relation to said tamper-resistant security device.

31. The user terminal according to claim 30, wherein the security conditions reflect at least one of the environment in which said security device is operated, the network interface over which a request for AKA processing comes, and the network used by the user terminal for network communication.

32. The user terminal according to claim 30, wherein said security policy processing includes at least one of a security policy decision process and a security policy enforcement process.

33. The user terminal according to claim 30, wherein said means for performing security policy processing is implemented in said tamper-resistant security device and configured for selectively disabling direct access to said AKA module.

34. The user terminal according to claim 30, wherein said tamper-resistant security device comprises means for detecting security conditions in relation to said tamper-resistant security device.

35. The user terminal according to claim 30, wherein said user terminal comprises means for detecting security conditions in relation to said tamper-resistant security device.

36. The user terminal according to claim 26, wherein said cooperating application is a security enhancing application, and said security device further comprises means for transferring a request for AKA processing directly to said AKA module if said security device is operated in an environment considered secure, and means for transferring said request to said security enhancing application if said security device is operated in an environment considered insecure.

37. The user terminal according to claim 26, wherein said cooperating application includes a security enhancing application, and said user terminal further

comprises means for transferring a request for AKA processing directly to said AKA module if said request comes over an interface considered secure, and means for transferring said request to said security enhancing application if said request comes over an interface considered insecure.

38. The user terminal according to claim 37, wherein said security enhancing application comprises a number of different security enhancing modules, and said security enhancing application is configured for selecting among said security enhancing modules in dependence on the type of interface.

39. The user terminal according to claim 26, wherein said cooperating application is a software application installed in an application environment of said tamper-resistant security device.

40. The user terminal according to claim 26, wherein said cooperating application includes a security enhancing application configured for authenticating a network over which said user terminal intends to communicate.

41. A network server managed by a trusted party sharing a security key with a tamper-resistant security device implemented in a user terminal, said tamper-resistant security device having an Authentication and Key Agreement (AKA) module for performing an AKA process with said security key,

wherein said network server comprises means for downloading a software application adapted for interfacing and cooperating with said AKA module into an application environment of said tamper-resistant device.

42. The network server according to claim 41, wherein said download application is at least one of a security enhancing application and a privacy enhancing application.

43. The network server according to claim 42, wherein said download application includes a security enhancing application combined with at least one security policy.
